Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1. (currently amended) A method of generating a shared key by a first correspondent in an MQV key generation protocol, wherein said key is computable by a second correspondent, said method comprising the steps of:
a) said first correspondent making a first short term public key available to said second correspondent over a communication channel;
b) said first correspondent obtaining a second short term public key from said second correspondent;
c) said first correspondent computing a first exponent derived from a first short term private key, said first short term public key, and a first long term private key;
d) said first correspondent computing a second exponent derived from said first short term private key, said first short term public key, a second short term public key and said first long term private key;
e) said first correspondent computing a first simultaneous exponentiation of said first exponent with said second short term public key and said second exponent with a second long term public key; and
f) said first correspondent using the results of said first simultaneous exponentiation to generate said shared key.

2. (currently amended) The method of claim 1 further comprising the steps of:
g) said second correspondent making said second short term public key available to said first correspondent over said communication channel;
h) said second correspondent obtaining said first short term public key from said first correspondent;
i) said second correspondent computing a [[third]] one exponent derived from a second short term private key, said second short term public key, and a second long term private key;

j) said second correspondent computing [[a fourth]] another exponent derived from said second short term private key, said second short term public key, said second long term private key, and said first short term public key;

k) said second correspondent computing a second simultaneous exponentiation of said [[third]] one exponent with said first short term public key and said [[fourth]] another exponent with a first long term public key; and

l) said second correspondent using the results of said second simultaneous exponentiation to generate said shared key.

3. (previously presented) The method of claim 2 wherein steps a) and g) are performed in parallel, steps b) and h) are performed in parallel, steps c) and d) are performed in parallel with steps i) and j), and steps k) and l) are performed in parallel with steps e) and f).

4. (previously presented) The method of claim 1 wherein said simultaneous exponentiation is performed by:

- establishing a window of width *w*;
- establishing a table of small exponentiations of said second short term public key, and a table of small exponentiations of said second long term public key to provide a series potential exponentiations representing said first and second exponents; and
- examining said tables using said window *w* until said shared key is computed.

5. (previously presented) The method of claim 4 wherein said step of examining said tables includes retrieving the corresponding powers of values of said second short term public key and said second long term public key within said window *w*, accumulating the product of corresponding entries from said tables and squaring said product *w* times, and examining further windows repeatedly until said shared key is computed.

6. (previously presented) The method of claim 1 wherein said simultaneous exponentiation is performed by:

- storing values of said first and second exponents in first and second registers respectively, each register having an associated pointer;

- using said pointers selectively accumulate and multiply corresponding values stored in said registers; and
- repeatedly multiplying said values until said shared key is computed.

7. (previously presented) The method of claim 1 implemented in an elliptic curve cryptosystem.

8. (previously presented) The method of claim 7 wherein said simultaneous exponentiation includes simultaneous multiple scalar multiplication using a window of width *w*, and tables of small exponentiations of said second short term public key and said second long term public key.